APPARATUS AND METHOD FOR INTELLECTUAL PROPERTY PROTECTION USING THE MICROPROCESSOR SERIAL NUMBER

Gene A. Frantz

1. Field of the Invention

This invention relates generally to microprocessors and, more particularly, to the protection of intellectual property such as software programs that are executed by the microprocessors.

2. Background of the Invention

As microprocessors have increased in speed of execution of instructions, the need for timely program execution implemented in the design of the processor itself, has diminished. The program execution functionality can therefore be implemented in software rather than in the hardware implementation. The placement

of increasing amount of intellectual property content in the software programming has the advantage of flexibility in the ability to change and/or update the operation of a data processing unit. However, the placement of increasing amounts of intellectual property in the software programs has made the protection of the software program increasingly important.

While software programs are usually provided under license and/or under copyright, the protection of software by contractual methods and/or copyright has proven largely been effectual. The ease of copying software program has lead to wide-spread violation of the intellectual property rights. Encryption methods have provided some relief when the encryption procedure and the encryption key can be separately provided to the user. Aside from the practical problem of trying to provide a decryption procedure and a decryption key to the user in manner to that is convenient for the user and difficult for a potential thief, once the procedure is determined by a potential thief, the entire data processing unit base is then open to comprise.

A need has therefore been felt for apparatus and an associated method to protect the intellectual property in a software program. It would be yet another feature of the apparatus and associated method to couple a software program with a processor or group of processors. It is a more particular feature of the apparatus and associated to

provide an encrypted software program using an encryption key associated with the processing unit to be used in executing the software program. It is a still more particular feature of the apparatus and associated method that at least a portion of the encryption key of an encrypted software program is derived from an identifying number stored in the processing unit that is to execute the software program. It is yet a more particular feature of the apparatus and associated method to provide an encryption key based on the serial number of a data processing system.

Summary of the Invention

The aforementioned and other features are accomplished, according to the present invention, by providing each processor with an identifying/serial number. The identifying/serial number is stored in a protected memory accessible only to the associated processor. For at least selected software programs to be executed by the processor, each software program is encrypted using at least a portion of the identifying/ serial number of the processor on which the program is to be executed as the decryption key. The encrypted software programs can be stored in the processor memory unit or external to the processor. When the software program is executed by the processor, the decryption procedure and the identifying/serial number are accessed by the processor and

used to decode the decrypted software program. The processor then executes the decrypted software program.

Other features and advantages of the present invention will be more clearly understood upon reading of the following description and the accompanying drawings and claims.

Brief Description of the Drawings

Figure 1 is block diagram of illustrating the relationship of an encrypted software program to the processing unit according to the present invention.

Figure 2 is flow chart illustrating the execution of an encrypted software program according to the present invention.

Description of the Preferred Embodiment

1. Detailed Description of the Drawings

Referring to Fig. 1, the relationship of an encrypted software program to the processing unit upon which software program will be executed is shown according to the present invention. A data processing unit 10 includes an input/output unit 15 for exchanging data, program, and control signals between external apparatus and the

processor 11. (As will be clear to those skilled in the art, the architecture of a data processing unit is typically more complicated than this discussion would indicate. For example, a direct memory access unit can transfer signals between the input/output unit 15 and the memory unit 13 without accessing the processor 11.) The processor 11 exchanges signal with the input/output unit 15, a memory unit 13 and a non-volatile memory unit 14. The memory unit typically includes the decryption program 131 and encrypted files 132. The protected, non-volatile memory 14 can store the identifying/serial number 141. Or the identifying/serial number can be hard-wired in the apparatus associated with processor 11. The identifying/serial number is accessible only to the data processing unit 10 with which it is associated. In addition, encrypted files 17A can be stored in an external memory unit 17 and applied to the processor 11.

Referring to Fig. 2, the procedure for implementation of providing a secure software program protocol according to the present invention. In step 201, an identifying/serial number is stored in a non-volatile memory in the data processing unit. The identifying/serial number can be hard-wired in the data processing unit integrated circuit according to one embodiment. In the memory unit 13, a decryption procedure that operates using at least a portion of the identifying/serial number as an encryption key is stored in the memory unit 13 in step 202.

In step 203, a software program is encrypted using the encryption procedure related to the decryption procedure of step 202. The encryption procedure uses the identifying/serial number as the encryption key. The encrypted software program is stored in the memory unit 13 in step 204. In step 205, in response to program requirements in the data processing unit 10, the decryption procedure, the encryption key and a selected encrypted program is transferred to the processor 11. The processor 11 then converts the encrypted program into executable text. In step 207, the processor 11 executes the decrypted software program.

2. Operation of the Preferred Embodiment

The present invention couples an encrypted software program with a processor or group of processors upon which the software program is to be executed. The coupling is accomplished by providing a microprocessor or group of microprocessors with an identifying/serial number. A software program is encrypted using at least at least a portion of the identifying/serial number as a key. The identifying/serial number is typically "hard-wired" in the microprocessor, but can be stored in a secure, non-volatile memory such as flash memory accessible only by the associated processor. In this manner, the software program can be used/decrypted only when the encryption of the software program is performed with the identifying/serial

number. This procedure has the advantage that the encrypted program can not be shared with another data processing unit. In addition, if the procedure were pirated, the procedure would be traceable to a specific device.

While the embodiment of the invention discussed above involved an encrypted software program being stored in the memory unit, it will be clear that the encrypted program can be stored in a location external to the data processing unit. The encrypted software program from an external program can be decrypted on the fly or block by block, or completely decrypted and the decrypted portion of the program stored in a protected memory unit accessible only to the associated processor. Similarly, the decrypted program can be executed on the fly or stored in a protected, internal memory for latter use either block by block or in its entirety.

The identifying/serial number is typically included in an integrated circuit processor. This identifier/serial number is typically used to provide information to the manufacturer in the event that the integrated circuit is defective. The identifier, that is typically associated with the date and parameters of the circuit parameter can be used to determine whether the defect is a result of the process itself or arises from some random factor. As will

be clear, a plurality of processing units can have the same serial number or identifying number assigned thereto.

One technique for using the present invention is for the manufacture/agent to have a list of identifying/serial numbers associated with the identity of the user of the target processor. In this manner, the manufacturer/agent can customize the encryption of files for the requesting user. A further level of security can e achieved by storing the identifying/serial numbers in a file addressed by a user identification, but capable of being accessed only by the encrypting apparatus.

While the invention has been described with respect to the embodiments set forth above, the invention is not necessarily limited to these embodiments. Accordingly, other embodiment variations, and improvements not described herein, are not necessarily excluded from the scope of the invention, the scope of the invention being defined by the following claims.